UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information Associated With:
JOHNMAY041994@GMAIL.COM
THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE, INC.,

Case No. **1:23-MJ-00218**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A-1

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B-1

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2252 and/or 2252A	Activities Relating to Material Involving the Sexual Exploitation of Minors

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

WESLEY DUNN Digitally signed by WESLEY DUNN Date: 2023.03.23 09:25:40 -04'00'

Applicant's signature

Wesley Dunn, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by FaceTime video conference *(specify reliable electronic means)*.

Date: **Mar 23, 2023**

Stephanie K. Bowman

Judge's signature

City and state: Cincinnati, Ohio

Hon. Stephanie K. Bowman, U.S. Magistrate Judge

Printed name and title

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information associated JOHNMAY041994@GMAIL.COM **(**TARGET ACCOUNT**)** that is stored at premises owned, maintained, controlled, or operated by the web-based electronic mail service provider known as Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Google Inc., (PROVIDER)

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. The contents of all emails associated with the account from account creation to present, including stored or preserved copies of emails sent to and from the account, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the PROVIDER and any person regarding the accounts, including contacts with support services and records of actions taken.

f. All other records of communications and messages of any kind made or received by the user, including all private or instant messages, and specifically including all attachments to any messages in their native formats (for example, if a .zip file was sent to another user, the .zip file shall be provided), history of communications of any kind, video calling history, pending "Friend" requests, and where such records exist, the identity of any other user or account with which a TARGET ACCOUNT was connected;

g. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, the PROVIDER shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

h. All search history, web history, Google Web & App Activity or Google "History Events" by the user of the TARGET ACCOUNT, including web clicks;

i. All web browsing activities that are identifiable with the TARGET ACCOUNT or with machine cookies used to access the TARGET ACCOUNT;

j. All records (including content records) pertaining to any Google service associated with the TARGET ACCOUNT, including services such as Gmail, Android, Developer Consoles, Android Market (including payment information), Google Play (including payment information), Google Analytics, Google Groups, Google Dashboard, Google Code, Google Chrome Sync, Kr Age Adult, Location History, Google Maps, Lock SafeSearch, Google Reader, Google Translate, Google Translator Toolkit, Google Talk, Blogger, Google Calendar, Google Docs, Google Drive, Google News, Google Reader, Google Services, Google+, Has

Google Profile, Has Plusone, Picasa Web Albums, YouTube, Tasks, iGoogle, Web History, and Hangouts;

k. For any Android Device associated with any TARGET ACCOUNT, all subscriber records, transactional information, search query history, browsing history, machine cookies, e-mail accounts ever linked to, Google Maps location information, Google Location history, application data from any Applications or "Apps," sensor data from the user's device that includes information on nearby Wi-Fi access points and cell towers, Face Unlock information (stored images), list of installed applications, operating system versions, phone numbers, International Mobile Station Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), call logs, stored text messages, voicemails, stored photos, contacts lists, favorites lists, synced Twitter/Facebook accounts, device information (serial numbers, make, model), clock and calendar time zone settings, stored memos and notes, device security settings, and any files associated with any TARGET ACCOUNT;

l. All other records and information, including:

a. All IP logs, including all records of the IP addresses that logged into the account;

b. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, authentication logs, telephone caller identification records, and locations;

c. any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP

protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning web sites navigated to, other e-mail or social media accounts accessed, or analytics related to the TARGET ACCOUNT;

d. **Any and all cookies** used by any computer or web browser associated with the TARGET ACCOUNT, including the IP addresses dates and times associated with the recognition of any such cookie;

e. All subscriber information pertaining to the TARGET ACCOUNT, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account including recovery/alternate e-mail addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred;

f. All subscriber information pertaining to **any other account associated with the cookie(s) associated the TARGET ACCOUNT,** including accounts associated because they share a common SMS or phone number in subscriber records,

including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account including recovery/alternate e-mail addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records; and

g. All subscriber information pertaining to any other account associated/related with the TARGET ACCOUNT (including Google accounts associated in any way with the IMEI/Android IDs identified in Attachment A), including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account including recovery/alternate e-mail addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records;

h. All records related to authenticating the user of the TARGET ACCOUNT, including use of two-factor authentication or App passwords used to allow access via a mobile device and the identity of those devices accessing the TARGET ACCOUNT;

i. Any information identifying the device or devices used to access any TARGET ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifiers, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access each TARGET ACCOUNT or other device-specific information; and

j. Any information showing the location of the user of a TARGET ACCOUNT, including while sending or receiving a message using a TARGET ACCOUNT or accessing or logged into a TARGET ACCOUNT.

The PROVIDER is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) - distribution or receipt of child pornography, and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography involving the user of Gmail account **johnmay041994@gmail.com** from account creation to present, including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

(a) Any information and or images/videos which visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

(b) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(c) The identity of the person(s) who communicated with the user ID about matters relating to sexual exploitation of children, the distribution or receipt of child pornography, or the possession of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH JOHNMAY041994@GMAIL.COM KIK ACCOUNT: GAMBIT104 THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE, INC., AND MEDIALAB, INC.	Case No. **1:23-MJ-00218** **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Wesley Dunn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, Inc., ("Google") headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 and certain accounts that are stored at premises owned, maintained, controlled, or operated by MediaLab, Inc., an electronic communications service provider headquartered at 1237 7th St., Santa Monica, CA 90401. The information to be searched is described in the following paragraphs and in Attachment A-1 and A-2. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, and MediaLab Inc., to disclose to the government records and other information (including the content of communications) further described in Section I of Attachment B-1 and B-2. Upon receipt of the information described in Section I of Attachment B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachment B1 and B-2.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since August 2020 and am currently assigned to the Cincinnati Division. Prior to my current position, I was employed for three years as a patrol officer for the Owensboro Police Department located in Owensboro, Kentucky. While employed by the Federal Bureau of Investigation, I have investigated federal criminal violations related to high technology or cybercrime, identity theft and credit card fraud. I have gained experience through training at the Federal Bureau of Investigation and everyday work relating to conducting these types of investigations. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and/or 2252A have been committed by Kik user gambit104 (believed to be Nicholas Bonavita). There is also probable cause to search the information described in Attachment A-1 and A-2 for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B-1 and B-2.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

OVERVIEW OF KIK MESSENGER & THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN'S CYBERTIPLINE PROGRAM

Kik Messenger Application

6. The following information has been provided to me from the Kik Law Enforcement Guide (dated February 26, 2020), online research that I have conducted, from other law enforcement officers, as well as my training and experience. Kik Messenger, commonly called Kik, is a freeware instant messaging mobile app from the Canadian company Kik Interactive, and available free of charge on iOS and Android operating systems. It is a social networking application that permits a user to trade and disseminate various forms of digital media while using a cellphone. Kik advertised itself as "the first smartphone messenger with a built-in browser." Kik was founded in 2009 and according to its company website was designed to "break down barriers [between operating systems] that would allow users to chat with whoever, whenever." In October 2019, Kik Interactive was purchased by Santa Monica, California based MediaLab Inc. MediaLab Inc. is a holding company that owns other internet-based communication applications such as Whisper, Datpiff and others.

7. Kik Messenger is a feature within Kik that allows its users to communicate with selected persons as well as browse and share any website content with those whom the user

selects while still within the Kik platform. Unlike other messaging apps, Kik usernames – not phone numbers - are the basis for Kik user accounts. Kik usernames are unique; can never be replicated; can never be changed, may include lower and uppercase letters, numbers and/or 4 periods and underscores; and will never contain spaces, emoticons or special characters. A Kik username is the only publicly available identifier MediaLab Inc. can use to identify a Kik account to law enforcement. The company cannot identify users using phone numbers, first and last name (display name), or email address.

8. In addition, Kik features include more than instant messaging. Kik users can exchange images, videos, sketches, stickers and even web page content by posting such content privately with individual users (with whom the user selects) or publicly (on the Kik platform) with multiple individuals who belong to "Groups." Groups are formed when like-minded individuals join collectively online in an online forum, created oftentimes by a Kik user designated as the Kik "Administrator" of the group. Groups can hold up to 50 Kik usernames. Groups are created to host/discuss topics such as modern popular culture-themed ideas as well as illicit/illegal-themed ideas. Public groups names are a user-generated hashtag; can never be replicated; can never be changed; may include lower and uppercase letters, numbers and/or periods and underscores; will never contain spaces, emoticons or special characters; The group hashtag will begin with a hash (#) (i.e.#AffidavitForWarrant).

The National Center for Missing and Exploited Children's CyberTipline Program

9. The National Center for Missing and Exploited Children (NCMEC) was incorporated in 1984 as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited children's issues.

10. NCMEC operates the CyberTipline, a system that allows for the general public, law enforcement, private companies such as Kik, and others to report potential sexual abuse issues to NCMEC. As part of the submission process, NCMEC informs those that report that information submitted via the CyberTipline will be shared with law enforcement for possible investigation.

PROBABLE CAUSE

11. On December 13, 2022, Kik submitted a cyber-tip to the CyberTipline. Kik's cyber-tip was assigned CyberTipline report number 141507188. Report 141507188 indicated that on December 11, 2022, Kik user **gambit104** (gambit) was reported for sharing apparent child pornography. Kik conducted a review and discovered private messages sent from gambit to an unknown user. The private messages, sent on December 04, 2022 contained thirteen individual video files. A Kik employee reviewed the videos and determined them to be child pornography. The following account information was included in Kik's cyber-tip:

a. Email address: johnmay041994@gmail.com

b. Screen/User Name: gambit104

c. ESP User ID: gambit104_coo

d. IP Address: 75.185.241.70 (Login).

12. NCMEC conducted a review of the thirteen video files submitted in Kik's NCMEC cyber-tip. The review indicated that ten of the videos depicted "apparent child pornography," two were "child pornography (unconfirmed)" and one depicted an unclothed child.

13. A grand jury subpoena was served on Charter Communications Inc. to provide subscriber information pertaining to IP address 75.185.241.70 and the associated date/time when

it was used to log into the gambit104 Kik account. On January 27, 2023, Charter Communications Inc. responded with the following information:

Target Details: IP 75.185.241.70

Subscriber Name: Nicholas Bonavita

Subscriber Address: 3956 Fulton Grove Rd, Cincinnati, OH 45245

Username: bbonavita62@yahoo.com, bonavita6162@charter.net

Phone Number: N/A

14. On March 13, 2023 an administrative subpoena was served on Kik Interactive for the IP address 75.185.241.70. On March 14, 2023, Kik Interactive responded with the following information:

First Name: Joe

Last Name: Bon

Account Created: 2022/11/06 21:46:06

User Location: IP: 75.185.241.70

Email: **johnmay041994@gmail.com** (unconfirmed)

Username: **gambit104**

Device Info: Nokia N152DL

15. From the response, it appears that Kik user gambit104 provided the email address johnmay041994@gmail.com during the initial registration for the account. Kik regularly uses the email address provided during registration to correspond with the registrant about their account and can be used for various functions such as conducting a password reset. The email address, johnmay041994@gmail.com, provided by Kik is listed as unconfirmed. "Unconfirmed" means that verification link contained within the initial activation email sent by Kik to

johnmay041994@gmail.com was not used. A Kik user's account being unconfirmed does not limit that user's ability to use or access Kik messenger functions.

16. An open-source database search revealed that 3956 Fulton Grove Rd, Cincinnati, Ohio 45245 is listed as Nicholas Bonavita's current residential address. Records indicate that Bonavita has lived at this address since approximately September 2021. Bonavita entered a plea of guilty to Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) in United States District Court for the Southern District of Ohio, in Case No. 1:21-cr-00124-TSB. He is currently awaiting sentencing.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

17. Most individuals who collect child pornography are sexually attracted to children, as their sexual arousal patterns and erotic imagery focus, in part or in whole, on children. The collection may be exclusively dedicated to children of a particular age/gender or it may be more diverse, representing a variety of sexual preferences involving children. Collectors of child pornography express their attraction to children through the collection of sexually explicit materials involving children, as well as other seemingly innocuous material related to children.

18. The above-described individuals may derive sexual gratification from actual physical contact with children, as well as from fantasy involving the use of pictures or other visual depictions of children or from literature describing sexual contact with children. The overriding motivation for the collection of child pornography may be to define, fuel, and validate the collector's most cherished sexual fantasies involving children.

19. Visual depictions may range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude depictions of children engaged in explicit sexual activity. In addition to child pornography, these individuals are also highly likely to collect other

paraphernalia related to their sexual interest in children. This other material is sometimes referred to as "child erotica," further defined as any material relating to children that serves a sexual purpose for a given individual. "Child erotica" is broader and more encompassing than child pornography, though at the same time the possession of such corroborative material, depending on the context in which it is found, may be behaviorally consistent with the offender's orientation toward children and indicative of his/her intent. "Child Erotica" includes things such as fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, cartoons and non-sexually explicit visual images.

20. Child pornography collectors often reinforce their fantasies by taking progressive, overt steps aimed at turning such fantasy(ies) into reality in some, or all, of the following ways: collecting and organizing their child-related material; masturbating while viewing child pornography; engaging children, online and elsewhere, in conversations, sometimes sexually explicit conversations, to fuel and fortify the fantasy; interacting, both directly and indirectly, with other like-minded adults through membership in organizations catering to their sexual preference for children, thereby providing a sense of acceptance and validation within a community; gravitating to employment, activities and/or relationships which provide access or proximity to children; and frequently persisting in the criminal conduct even when they have reason to believe the conduct has come to the attention of law enforcement. These are need driven behaviors to which the offender is willing to devote considerable time, money, and energy in spite of risks and contrary to self-interest.

21. Child pornography collectors almost always maintain and possess their material(s) in the privacy and security of their homes or some other secure location, to include Internet cloud storage. The collection may include sexually explicit or suggestive materials

involving children, such as photographs, magazines, narratives, motion pictures, video tapes, books, slides, drawings, computer images or other visual media. The collector is often aroused while viewing the collection and, acting on that arousal, he/she often masturbates, thereby fueling and reinforcing his/her attraction to children.

22. Due to the fact that the collection reveals the otherwise private sexual desires and intent of the collector and represents his most cherished sexual fantasies, the collector rarely disposes of the collection. The collection may be culled and refined over time, but the size of the collection tends to increase. Individuals who use a collection in the seduction of children or to document the seduction of children treat the materials as prized possessions and are especially unlikely to part with them. Even if a child pornography collector deletes files from his hard drive or other electronic media, a computer expert is often able to retrieve those files using computer forensic tools.

BACKGROUND CONCERNING EMAIL

23. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allow subscribers to obtain email accounts at the domain names gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google ask subscribers to provide basic personal information. Therefore, the computers of the Google are likely to contain stored electronic communications (including retrieved and un-retrieved email for the Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience,

such information may constitute evidence of the crimes under investigation because the information can be used to identify the accounts' user or users.

24. In my training and experience, Google generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

25. In my training and experience, Google typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

26. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as

technical problems, billing inquiries, or complaints from other users. Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

27. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, Google typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*,

location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

28. Based on the foregoing, I submit that there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and/or 2252A have been committed by Kik user gambit104. I respectfully request that the Court issue the proposed search warrant authorizing the search of the accounts described in Attachments A-1 and A-2 and the seizure of items described in Attachments B-1 and B-2.

29. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google and MediaLab, Inc. Because the warrant will be served on these providers, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

30. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents

because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

WESLEY DUNN Digitally signed by WESLEY DUNN
Date: 2023.03.23 09:26:13 -04'00'

Wesley Dunn
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on March 23, 2023 by reliable electronic means, specifically, FaceTime video conference.

Stephanie K. Bowman

HONORABLE STEPHANIE K. BOWMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to Be Searched

This warrant applies to information associated JOHNMAY041994@GMAIL.COM **(**TARGET ACCOUNT**)** that is stored at premises owned, maintained, controlled, or operated by the web-based electronic mail service provider known as Google, Inc., headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by Google Inc., (PROVIDER)

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of the PROVIDER, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the PROVIDER, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the PROVIDER is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

a. The contents of all emails associated with the account from account creation to present, including stored or preserved copies of emails sent to and from the account, draft emails, deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the PROVIDER and any person regarding the accounts, including contacts with support services and records of actions taken.

f. All other records of communications and messages of any kind made or received by the user, including all private or instant messages, and specifically including all attachments to any messages in their native formats (for example, if a .zip file was sent to another user, the .zip file shall be provided), history of communications of any kind, video calling history, pending "Friend" requests, and where such records exist, the identity of any other user or account with which a TARGET ACCOUNT was connected;

g. All stored passwords, including passwords stored in clear text and hash form, and for any hashed values that include a salt, the PROVIDER shall provide the salt value used to compute the stored password hash value, and any security questions and answers;

h. All search history, web history, Google Web & App Activity or Google "History Events" by the user of the TARGET ACCOUNT, including web clicks;

i. All web browsing activities that are identifiable with the TARGET ACCOUNT or with machine cookies used to access the TARGET ACCOUNT;

j. All records (including content records) pertaining to any Google service associated with the TARGET ACCOUNT, including services such as Gmail, Android, Developer Consoles, Android Market (including payment information), Google Play (including payment information), Google Analytics, Google Groups, Google Dashboard, Google Code, Google Chrome Sync, Kr Age Adult, Location History, Google Maps, Lock SafeSearch, Google Reader, Google Translate, Google Translator Toolkit, Google Talk, Blogger, Google Calendar, Google Docs, Google Drive, Google News, Google Reader, Google Services, Google+, Has

Google Profile, Has Plusone, Picasa Web Albums, YouTube, Tasks, iGoogle, Web History, and Hangouts;

k. For any Android Device associated with any TARGET ACCOUNT, all subscriber records, transactional information, search query history, browsing history, machine cookies, e-mail accounts ever linked to, Google Maps location information, Google Location history, application data from any Applications or "Apps," sensor data from the user's device that includes information on nearby Wi-Fi access points and cell towers, Face Unlock information (stored images), list of installed applications, operating system versions, phone numbers, International Mobile Station Equipment Identity (IMEI), Mobile Equipment Identifier (MEID), call logs, stored text messages, voicemails, stored photos, contacts lists, favorites lists, synced Twitter/Facebook accounts, device information (serial numbers, make, model), clock and calendar time zone settings, stored memos and notes, device security settings, and any files associated with any TARGET ACCOUNT;

l. All other records and information, including:

a. All IP logs, including all records of the IP addresses that logged into the account;

b. All user connection logs and transactional information of all activity relating to the TARGET ACCOUNT, including all log files, dates, times, durations, data transfer volumes, methods of connection, IP addresses, ports, routing information, dial-ups, authentication logs, telephone caller identification records, and locations;

c. any and all logs of user activity and user agent string, including: web requests or HTTP requests; any logs containing information such as the Requestor's IP address, identity and user ID, date and timestamp, request URI or URL, HTTP

protocol version, referrer, and other user agent string information; login tracker logs; account management logs; and any other information concerning web sites navigated to, other e-mail or social media accounts accessed, or analytics related to the TARGET ACCOUNT;

d. **Any and all cookies** used by any computer or web browser associated with the TARGET ACCOUNT, including the IP addresses dates and times associated with the recognition of any such cookie;

e. All subscriber information pertaining to the TARGET ACCOUNT, including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account including recovery/alternate e-mail addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records, **and including any changes made to any subscriber information** or services, including specifically changes made to secondary e-mail accounts, phone numbers, passwords, identity or address information, or types of services used, and including the dates on which such changes occurred;

f. All subscriber information pertaining to **any other account associated with the cookie(s) associated the TARGET ACCOUNT,** including accounts associated because they share a common SMS or phone number in subscriber records,

including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account including recovery/alternate e-mail addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records; and

g. All subscriber information pertaining to any other account associated/related with the TARGET ACCOUNT (including Google accounts associated in any way with the IMEI/Android IDs identified in Attachment A), including the date on which the account was created, the length of service, the IP address used to register the account, the subscriber's full name(s), screen name(s), other account names or e-mail addresses associated with the account including recovery/alternate e-mail addresses, gender, date of birth, telephone numbers, physical addresses, and other identifying information regarding the subscriber, the types of service utilized, account status, account settings, login IP addresses associated with session dates and times, as well as means and source of payment, including detailed billing records;

h. All records related to authenticating the user of the TARGET ACCOUNT, including use of two-factor authentication or App passwords used to allow access via a mobile device and the identity of those devices accessing the TARGET ACCOUNT;

i. Any information identifying the device or devices used to access any TARGET ACCOUNT, including any Android ID, Advertising ID, unique application number, hardware model, operating system version, unique device identifiers, Global Unique Identifier or "GUID," serial number, mobile network information, phone number, device serial number, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access each TARGET ACCOUNT or other device-specific information; and

j. Any information showing the location of the user of a TARGET ACCOUNT, including while sending or receiving a message using a TARGET ACCOUNT or accessing or logged into a TARGET ACCOUNT.

The PROVIDER is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2) - distribution or receipt of child pornography, and 18 U.S.C. § 2252A(a)(5)(B) - possession of child pornography involving the user of Gmail account **johnmay041994@gmail.com** from account creation to present, including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

(a) Any information and or images/videos which visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

(b) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(c) The identity of the person(s) who communicated with the user ID about matters relating to sexual exploitation of children, the distribution or receipt of child pornography, or the possession of child pornography, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support

staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, Inc. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, Inc., and they were made by Google, Inc. as a regular practice; and

b. such records were generated by Google, Inc. electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature